Guarding Your Trade Secrets: Avoiding The Trap Door Into The Public Domain

William D. Grand

GREENBAUM, ROWE, SMITH, RAVIN, DAVIS & HIMMEL

Job changes today are common. Employers should be especially vigilant, therefore, to ensure that their marketing and manufacturing methods, customer lists, formulas, innovations and technology do not leave with an employee. Only a small portion of an employer's "intellectual property" is protected by statutes, such as patent and copyright statutes. The principal protection an employer has is through judicial enforcement of the common law of trade secrets.

What Are Trade Secrets?

The concept of a "trade secret" is a nebulous one. It has been characterized as a formula, process, plan, device or compilation, known by the employer but not generally known in the industry, and sought to be kept secret by the employer.

The *Restatement of Torts* lists six factors to determine whether a given idea or information is a trade secret: (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the owner to guard the secrecy of the information; (4) the value of the information to the business and to its competitors; (5) the amount of effort or money expended in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Conversely, the courts have established that trade secrets are not: (1) matters of public knowledge; (2) matters of general knowledge and/or skill within an industry; (3) routine or trivial difference in practices and/or methods; or (4) the facility, skill or experience learned during the course of an employee's employment. One court's definition of "trade secret" is often cited:

"A trade secret may consist of a formula, process, device or compilation which one uses in his business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. * * * Its subject matter must not be a matter of public knowledge or of general knowledge within the industry. * * * Although a substantial measure of secrecy must exist, the secrecy need not be absolute and disclosure to employees involved in its use will not ordinarily result in loss of the employer's protection. * * * Novelty and invention are not essential for the trade secret as they are for patentability. * * * And the fact that every ingredient is known to the industry is not controlling for the secret may consist of the method of combining them which produces a product superior to that of competitors." [1]

William D. Grand

Avoiding The Trap Door

Unlike patent protection, which relies upon a statutory scheme for legal protection, a company can legally protect its trade secrets only if it has taken affirmative steps to guard their secrecy. In other words, lack of vigilance is a "trap door" into the public domain.

While no particular procedure is mandated, a company should establish a written protocol for protecting its information. The protocol should include as many of the following as possible:

(1) *Confidential Designation On All Information That The Company Deems Proprietary.*

A company should have a policy of stamping its proprietary information "CONFIDENTIAL." This accomplishes two things: it communicates to employees that the information is not to be disseminated outside the company, and it communicates to a court that the company considered the information secret and attempted to guard it as such.

(2) *Written Confidentiality Agreements Signed By All Employees.*

The company should require every employee to sign a written confidentiality agreement, and should not distinguish in this requirement between research chemists, lab technicians, or machine operators, for example, because each at one time or another will have access to formulas, research projects, assay methodologies and manufacturing methods of the company.

The confidentiality agreement should, in clear, simple language, set forth the company's confidentiality requirements. The agreement should prohibit disclosure to persons outside the company. The agreement should explain the importance to the company of its proprietary information and the damage that will result if it is disclosed.

The company should institutionalize a follow up "reminder" program for all employees. On an annual basis, employees should be required to sign a statement that he or she has reread the confidentiality agreement previously executed, and will continue to abide by its terms.

(3) *Security.*

The company's protocol should outline security procedures that should be implemented and maintained. Two purposes are served — to limit the exposure of the information and to convince a court, if necessary, that the company viewed its information as sensitive and took steps to protect it.

Security measures should include keeping formulas, assay methods, research notebooks, and manufacturing instructions under lock and key when not in use; keeping laboratory doors and other rooms where sensitive information is stored locked at night; and removing formulas and manufacturing instructions from production rooms at night.

(4) *Limited Dissemination and Proper Designation of Sensitive Memorandum and Research Papers.*

Like formulas and laboratory notebooks, all sensitive memoranda and research papers or reports that are circulated to other employees of the company should be disseminated only to those people who have a need to see them, and they should be stamped confidential. If the document is extremely sensitive, copies should be collected following dissemination and kept in a central place or safe under lock and key.

(5) *Monitoring FOIA Releases.*

A company often files sensitive information with a federal or state agency which has the potential of being disclosed by that agency pursuant to the Freedom of Information Act ("FOIA"). A company's protocol should include periodic checks to determine what information has been released by the agency and to whom. This will enable the company to monitor its competitors' efforts to obtain information from it, and, if the release appears to be unjustified under the criteria established under the FOIA, the company can lobby the agency, and sue, if necessary, to prevent a reoccurrence of unwarranted disclosures.

(6) *Confidentiality Agreements With Suppliers.*

Suppliers of raw materials often maintain extensive files of formulas and other information related to the use of their raw materials. Companies will sometimes notify suppliers of their new product plans to elicit from them assistance and information.

Confidentiality agreements with the suppliers are essential. The agreements should contain a statement that the company's new product plans are confidential and a promise of nondisclosure. The consideration for the promise, actual or possible business, should be recited.

(7) *Cost Accounting.*

Establishing a trade secret may require proving that substantial costs were involved to develop the information. For this reason, the better the cost accounting system established by the company to record its costs for each project, the easier its proofs will be to establish trade secret status.

Court Remedies

Injunctive relief is a recognized remedy in trade secret cases. Courts in trade secret cases adhere to the standard test for determining whether preliminary injunctive relief is appropriate: Is plaintiff likely to succeed on the merits? Are money damages inadequate? Does the threatened injury to plaintiff outweigh the harm an injunction may cause to the defendant? Unless each of these questions is answered affirmatively, a court will probably not grant preliminary injunctive relief.

Where the trade secret is novel, a court may grant a permanent injunction at the conclusion of the case, but courts tend to weigh the harm of the misappropriation carefully and limit the injunction in time and scope accordingly.

Money damages may also be awarded. Courts have relied upon at least three bases to calculate damages: plaintiff's lost profits, defendant's actual profits, and plaintiff's development costs.

Lost profit damages are often based upon the number of sales made by the defendant multiplied by the plaintiff's profit margins. In determining the plaintiff's profit margin, courts will commonly ignore fixed overhead expenses, reasoning that plaintiff's additional sales would not have generated additional fixed overhead expenses.

Some courts have measured damages based upon the defendant's profits. The theory is that the plaintiff is entitled to restitution based upon unjust enrichment, or that the plaintiff is entitled to an accounting for profits because of the defendant's breach of fiduciary duty.

For what period should plaintiff's lost profits or defendant's profits be assessed? It has been suggested that where the defendant acquired the information without knowledge of its trade secret status, the period of liability does not commence until notice is received, and its duration is a function of the ability of the defendant to have acquired the information independently. This "headstart" rule was developed by the courts to limit the damages suffered by the plaintiff to the period the defendant was in the market because of the "headstart" accorded it by the secret information.

However, in some cases the courts have held these measures to be inadequate, and have required defendants to pay to the plaintiff all or a portion of plaintiff's development costs. This third measure of damages has been most frequently applied where development costs were particularly high in comparison to the profits earned from the trade secret, and has been awarded in some cases in addition to damages calculated on the basis of lost profits.

Conclusion

Trade secret law affords significant protection, but only to companies that are diligent. A company should prepare now for a trade secret case by performing an internal audit to determine whether necessary protocols are being followed. Only then will a company ensure that a court will deem the company's secrets guarded, and therefore protected, information.

***William D. Grand** is a Litigation Partner in the Woodbridge, New Jersey, law firm of Greenbaum, Rowe, Smith, Ravin, Davis & Himmel. He specializes in trial practice and has tried cases in the federal and state courts of New York and New Jersey. His litigation experience includes a broad range of disputes, including trade secret, product liability, eminent domain, and environmental cases.*

[1] Sun Dial Corp. v. Rideout, *16 N.J. 252 (1954).*